



# **Recovering DRAM Functions**

Advisor: Carina Fiedler

#### Motivation

DRAM-based attacks, such as Rowhammer, require knowledge about how physical addresses are mapped to different DRAM banks and rows. Since only Intel initially documented these functions, reverse-engineering is required to recover the mapping on newer systems. DRAMA[1] and newer variations of the tool recover these functions via a timing side channel. However, these tools fail on some newer systems.

We will develop a framework that recovers the mapping from physical addresses to DRAM banks and rows and evaluate the tool on modern AMD and Intel systems.

## **Goals and Tasks**

- Get familiar with DRAMA[1].
- X Develop a framework to recover DRAM functions.
- Optional: Optimize speed of recovery.
- 🄀 Evaluate the tool on AMD and Intel.

### Literature

 P. Pessl et al. DRAMA: Exploiting DRAM Addressing for Cross-CPU Attacks doi.org/10.48550/arXiv.1511.08756

### **Courses & Deliverables**



## **Recommended if you're studying**

☑CS ☑ICE ☑SEM

#### Prerequisites

- > Interest in timing side channels, reverse-engineering, algorithms
- > Programming (C/C++)
- Information Security, Operating Systems

## **Advisor Contact**

carina.fiedler@tugraz.at